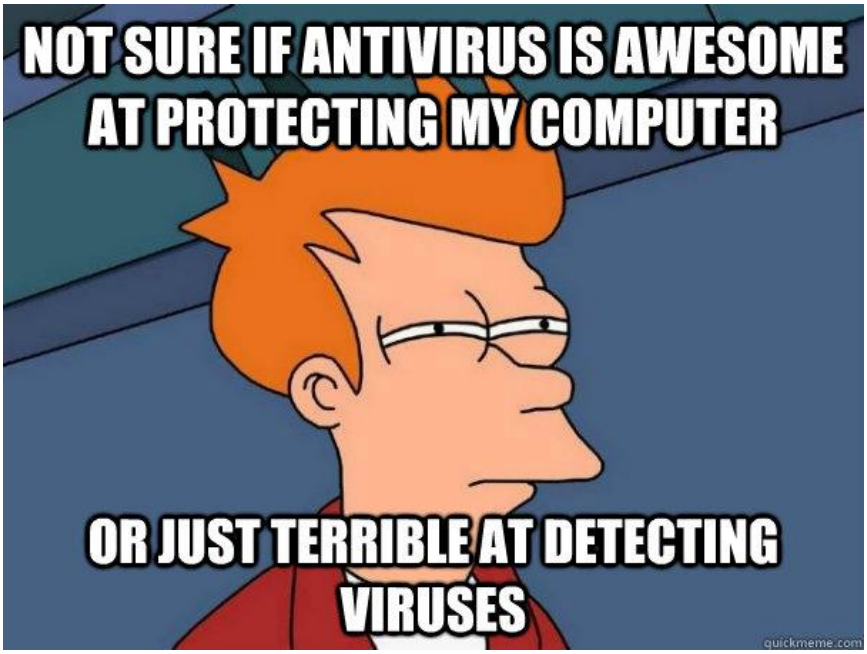

ASSIGNMENT 1

ITRI 625

ENRICO DREYER
31210783

Table of Contents

1. Introduction

In this report the network security of NWU Vaal in terms of networks will be discussed. The main topics will be the various threats, controls that are in place against the threats, firewalls used, intrusion detection systems that are in place and security aspects in terms of the e-mail system. Throughout the report recommendations will be made when necessary.

2. Various threats

According to Charles P. Pfleeger (2015) the four potential types of harm that NWU can experience is *interception*, *modification*, *fabrication* or *interruption*. Although the terminology is a bit different, these types still apply to networks. In terms of *interception*, it is often called wiretapping or eavesdropping, *modification* and *fabrication* is often called integrity failures and *interruption* is often called denial of service.

2.1. Interception

Interception is when an unauthorized party got access to an asset (genesisdatabase, 2010). This party can be a program, a person, or a computing system. Examples include obtaining data in a network (wiretapping). Loss can sometimes be detected easily, but a silent interceptor can leave no trace and no way of detecting interception. The best way to counter interception for NWU is by making use of a strong encryption (spamlaws, 2003).

2.2. Modification

According to genesisdatabase (2010), if a party that is unauthorized not only gains access to data, but also tempers with the data, it is called modification. For example, when someone changes values in the NWU database, or change functionality on efundi. This does not only apply to software, but hardware as well. According to Edwards (2018) some of the ways that NWU can prevent modification is to keep track of changes in the network, make use of atomization and to document network changes.

2.3. Fabrication

This is when an unauthorized party creates a fabrication of fake objects on a system. Examples include when a party inserts spurious transactions in NWU's network communication system. If skilfully done, they are almost impossible to distinguish from the real thing (genesisdatabase, 2010). According to Rasayely (2019), NWU can make use of certification of data and imposition of supervision on respondents.

2.4. Interruption

This is when an asset becomes unavailable, lost, or unusable. For NWU, this can be malicious destruction of hardware devices, malfunction of an operating system, erasure of data files or programs. According to Murray (2021) what NWU can do to detect interruption is to do constant speed tests, traceroute tests and ping tests.

3. Controls that are in place

NWU has network encryption in place to ensure that the network stays as safe as possible, this is in place to counter *interception*. Encryption is one of the most versatile and important tool in terms of network security (Charles P. Pfleeger, 2015). Encryption provides privacy, separation, integrity, and authenticity.

Another control that is in place is Bolster Access Control, this is making use of a strong password system. This is a very basic way of protecting the data of NWU, they make use of a mix of uppercase and lower-case letters, special characters, and numbers, as well as creating a strong access control policy.

NWU also keeps their software updated. This goes for anti-virus software to the operating systems of the computers. This can patch vulnerabilities in the security system. By making use of manual updates can be frustrating and time consuming, thus they make use of automatic software updates.

NWU makes use of standardized software, this means that you can not install any software without approval, they also reset the computers in the labs to wipe any applications or saved files that is not supposed to be on the computers.

Network Protection Measures that NWU follows include making use of Firewalls, IDS and IPS to follow up on potential packet floods, ensure proper access controls, virtual private networks, network segmentation and they conduct proper maintenance.

Along with all the controls that are in place, they also make sure that their employees are trained to understand what network security is, most of the external threats are caused by an insider act. They should also know who to contact in case of a security breach.

4. Firewalls used

A firewall is a device made to filter traffic between an inside or protected network and a less trustworthy network (Charles P. Pfleeger, 2015). There is usually a dedicated device that runs a firewall, as a single point through which traffic is sent, performance is important, so it takes some of the strain off the network.

Typically and most probably the firewall that NWU uses does not have loaders, compilers, debuggers, text editors or any other tools that an attacker might use to harm the firewall computer (Charles P. Pfleeger, 2015). The firewall is supposed to keep the environment safe from malicious software, for this there are policies that are designed to address when malicious things might happen.

NWU has different firewall types in place, for example a simple firewall makes judgements based on header data, this is called screening routers. Where there are more complex firewalls that look at specific communications to make decisions on accessibility (Hayajneh et al., 2013). In terms of NWU, simplicity is not always a bad thing, the security policy can be basic if the firewall protects against the threats that it is intended to counter.

The different firewalls include Packet Filter, Stateful Inspection, Application Proxy, Circuit Gateway, Guard and Personal Firewall. Each playing a role in protecting against specific threats.

Firewalls can protect NWU only if the firewall control the entire perimeter. This Firewall can not protect the data that is outside the perimeter. The firewall is one of the most visible part of a network, thus making it the most attacked target, this making use of multiple layers of security is essential for NWU.

5. Intrusion detection system

An intrusion detection system is usually another computer separate from the network, that obverses any activity to detect suspicious malicious events. At the NWU they have smoke alarms, that detect danger and activates the necessitates action. This alarm can call the fire department, alert the control team, sound an evacuation alarm, or active a sprinkler system.

In many cases the response is to alert a human team, this allows the team to decide what further actions to take. The IDS can also go into protection mode, this isolates a suspicious intruder then constraints further access, this is called an Intrusion Protection System (IPS).

The two types of intrusion detection systems are heuristic, and signature based. The Signature-based system performs pattern-matching to detect suspicious activity, reports the situation then links the report to the known attack type. Whereas the Heuristic system builds a model of behaviour that is acceptable and flag suspicious activity. An administrator can mark activities that they find acceptable, the system then adapts its model accordingly. This allows the Heuristic system to learn what is acceptable and not, as well as rates how dangerous the threat is.

These two styles of intrusion detection have different approaches, with their own advantages and disadvantages. For NWU, the IDS must be simple, fast, accurate and complete (detect attacks with negligible performance penalty).

6. Security aspects of the email system

Attackers use email to send software that is malicious to a user (Loshin, 2021). At NWU email is one of the predominant end-user network applications, thus making it one of the groups that attackers focus on to exploit email security threats. The security threats fall under the three general categories called Malware delivery, Phishing and Domain spoofing.

6.1. Malware delivery

File attachments are one of the main ways to deliver malware (Loshin, 2021). Ransomware can be spread in any network, but email became a natural fit, if an email account is leaked it can be used to send out more ransomware to different accounts. One way that NWU can counter this is to allow text only emails, and not allow attachments, but this makes it difficult for students and teachers to communicate. So, a different approach for NWU is to enable email filtering and monitoring systems.

6.2. Phishing

According to Loshin (2021) phishing is using an email to carry out social engineering campaigns to mislead a victim to perform an action. This leads to users giving personal information by clicking on harmful links. This can lead to important NWU information being leaked. They way NWU counters this is by making use of email filtering monitoring systems and making sure that the employees have the needed training and is aware of the potential threat.

6.3. Domain Spoofing

Spoofing domains is a well-known tactic to mislead users into believing an email came from a legitimate domain. For example, a fake efundi notification, that asks you to log in, this is a way of getting the personal information of important people form the NWU. The way NWU counters this type of email attacks can be tricky, by making use of monitoring systems can scan emails for domains that are legit and well known, and domains that are linked to persistent threat groups.

7. Conclusion

In this report the details of network communications and security and how they can apply to NWU was discussed. The main topics that were discussed were the various threats, controls that are in place against the threats, firewalls used, intrusion detection systems that are in place and security aspects in terms of the e-mail system.

8. References

Charles P. Pfleeger, S. L. P., Jonathan Margulies. (2015). *Security in computing*.

Edwards, J. (2018). Managing Network Configuration Changes: Five Best Practices. https://www.whatsupgold.com/blog/best-practices-in-network-configuration-and-change-management

genesisdatabase. (2010). *Types of threats | Interception | Interruption | Modification | Fabrication*. https://genesisdatabase.wordpress.com/2010/12/13/types-of-threats-interception-interruption-modification-fabrication/#:~:text=An%20interception%20means%20that%20some%20unauthorized%20party%20has,or%20wiretapping%20to%20obtain%20data%20in%20a%20network.

Hayajneh, T., Mohd, B. J., Itradat, A., & Quttoum, A. N. (2013). Performance and information security evaluation with firewalls. *International Journal of Security and Its Applications*, *7*(6), 355-372.

Loshin, P. (2021). The top 3 email security threats and how to defuse them. https://searchsecurity.techtarget.com/tip/The-top-3-email-security-threats-and-how-to-defuse-them

Murray, J. (2021). *How to Check for Internet Interruptions*. https://www.techwalla.com/articles/how-to-check-for-internet-interruptions

Rasayely. (2019). Data Fabrication/Falsification… Do Not Ever Do! https://www.rasayely.com/data-fabrication-falsification-do-not-ever-do/

spamlaws. (2003). *Types of Wireless Network Attacks: Interception*. https://www.spamlaws.com/interception-attack.html#:~:text=The%20best%20wireless%20security%20protection%20against%20interception%20exploits,can%20be%20cracked%20in%20under%20one%20minute%27s%20time.